Amendments to the Claims:

This listing of claims replaces all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Previously Presented) A communications system comprising:

at least one communications server associated with at least one communications network;

at least one communications terminal connected to the communications network to form a client-server relationship with the at least one communications server;

at least one policy definition point associated with said at least one communications server, said policy definition point defining policies for services, authentication, authorization, and accounting; and

at least one policy enforcement point associated with said at least one communications terminal, wherein said policy enforcement point is operable to enforce on said communications terminal the policies defined in said policy definition point.

2. (Cancelled)

3. (Previously Presented) The communications system according to claim 1, wherein said policy enforcement point includes means for enforcing policies pertaining to services, authentication, authorization and accounting.

4. (Previously Presented) The communications system according to claim 1, wherein said policy enforcement point resides in said at least one communications terminal as a local policy enforcement point.

5. (Previously Presented) The communications system according to claim 1, wherein said at least one communications terminal is operable to support several simultaneously ongoing independent client-server relationships.

6. (Previously Presented) The communications system according to claim 1, further comprising at least two mutually heterogeneous communication networks, wherein said at least one communications terminal is operable to exchange information with said at least two mutually heterogeneous communication networks.

7. (Previously Presented) The communications system according to claim 1, wherein said policy definition point is associated with at least one cluster of said at least one communications server.

8. (Previously Presented) The communications system according to claim 7, wherein said policy definition point includes means for enacting policies in said at least one cluster of servers.

9. (Previously Presented) The communications system according to claim 1, wherein said policy enforcement point includes means for enforcing a plurality of policies emanating from a plurality of networks and service providers.

10-11. (Cancelled)

12. (Previously Presented) The communications system according to claim 1, wherein said policy definition point includes a global location register indicating in which of said at least one communications network said at least one communications terminal resides.

13. (Previously Presented) The communications system according to claim 1, wherein said policy definition point further includes a subscriber database including means for storing subscriber IP addresses and encryption keys for each of a plurality of subscribers.

14. (Previously Presented) The communications system according to claim 1, further comprising a credential verifier providing means for anonymous payment of access for at least one of said at least one communications network.

15. (Previously Presented) The communications system according to claim 1, wherein said client-server relationship is provided by a transparent packet pipe transporting and classifying packets according to Quality of Service.

16. (Currently Amended) A method for global roaming in a communications system, said method comprising the steps of:

forming a client-server relationship between at least one communications terminal and at least one communications server associated with at least one communications network;

defining policies pertaining to services authentication, authorization, and accounting in a policy definition point within said communications network; and

enforcing the defined policies at a policy enforcement point associated with the communications terminal.

17. (Cancelled)

18. (Cancelled)

19. (Previously Presented) The method of claim 16, further comprising the step of defining, by said policy definition point, said policies in a plurality of server clusters.

20. (Cancelled)

21. (Previously Presented) The method of claim 16, further comprising the step of storing in said policy definition point subscriber IP addresses and encryption keys for each of a plurality of subscribers.

22. (Previously Presented) The method of claim 16, further comprising the step of providing said client-server relationship by transporting and classifying packets according to Quality of Service.

23. (Previously Presented) The method of claim 16, further comprising the step of providing separate charging mechanisms for access and services for client-server based transactions.

24. (Previously Presented) The method of claim 16, further comprising the step of defining a policy domain having multiple policy blocks, each containing a specific relationship between a client and said at least one communications server.

25. (Previously Presented) The method of claim 16, further comprising the steps of:

entering said policies in said policy enforcement point by a service provider; and

updating said policies.

26. (Withdrawn) A method for anonymous payment of a subscriber for a service of a network, said method comprising the steps of:

requesting a service by a subscriber using a mobile terminal;

transmitting encrypted payment information from the mobile terminal to an access node;

reading, by the access node, the encrypted payment information;

adding, by the access node, a transaction number to the encrypted payment information;

transmitting the encrypted payment information from the access node to a credential verifier server identified in the payment information;

decrypting, by the credential verifier server, the encrypted payment information;

verifying, by the credential verifier server, whether the decrypted payment information is correct;

transmitting the transaction number and a positive acknowledgment from the credential verifier server to the access node;

transmitting a message including an IP address and the positive acknowledgment from the access node to the mobile terminal; and

storing in a policy enforcement point the IP address associated with the service requested by the subscriber.

27. (Withdrawn) The method of claim 26, further comprising the step of the policy enforcement point enabling the service requested by the subscriber.

28. (Withdrawn) The method of claim 26, further comprising the steps of:

monitoring the transactions of the subscriber using the service; and

storing the transactions as accounting information.

29. (Withdrawn) The method of claim 26, further comprising the step of ending the requested service by transmitting an end session message.

30. (Withdrawn) The method of claim 26, further comprising the steps of:

sending the accounting information from the policy enforcement node to a secure mobile portal;

comparing the sent accounting information with accounting information generated in the secure mobile portal;

sending a positive accounting confirmation if the sent and generated accounting information correspond; and

sending a negative accounting confirmation if the sent and generated accounting information do not correspond.

31. (Withdrawn) A communications system comprising:

a policy definition point for defining policies for services, authentication, authorization, and accounting;

a policy enforcement point for enforcing the defined policies of a subscriber;

an access node for reading a credential verifier from a packet received from a mobile terminal, adding a transaction number to the credential verifier, and forwarding the packet to the credential verifier specified in the packet;

a credential verifier for granting access to a particular service requested from the mobile terminal; and

a communications network for transporting data between said policy definition point, said policy enforcement point, said access node, and said credential verifier.

32. (Withdrawn) the communications system of claim 31, wherein said policy enforcement point further comprises:

an authorization database for storing the policies defined in the policy definition point;

a policy enforcement point key for identifying the policy enforcement point to the policy definition point;

an authentication database for authenticating the subscriber and allowing access to the policy enforcement point; and

an accounting log for storing accounting information related to the service requested by the subscriber.

***